Proceedings Paper:
Kahrobaei, Delaram orcid.org/0000-0001-5467-7832, Tortora, Antonio and Tota, Maria (2020) Multilinear cryptography using nilpotent groups. In: Baginski, Paul, Fine, Benjamin, Moldenhauer, Anja, Rosenberger, Gerhard and Vladimir, Shpilrain, (eds.) Elementary Theory of Groups and Group Rings, and Related Topics:Proceedings of the Conference held at Fairfield University and at the Graduate Center, CUNY, November 1-2, 2018. Elementary theory of groups and group rings and related topics, 01 Nov 2018, Fairfield University. De Gruyter Proceedings in Mathematics . De Gruyter , USA , pp. 127-134.

https://doi.org/10.1515/9783110638387-013

Delaram Kahrobaei, Antonio Tortora, and Maria Tota

Multilinear cryptography using nilpotent groups

Abstract: In this paper, we develop a novel idea of multilinear cryptosystem using nilpotent group identities.

Keywords: Group based cryptotgraphy, multilinear cryptosystem, nilpotent group

MSC 2010: 20F18, 20F45

1 Introduction

In recent years, multilinear maps have attracted attention in cryptography community. The idea has been first proposed by Boneh and Silverberg [1]. For $n > 2$, the existence of n-linear maps is still an open question. One of the main applications of multilinear maps is their use for indistinguishability obfuscation. For example in [5], Lin and Tessaro proved that trilinear maps are sufficient for the purpose of achieving indistinguishability obfuscation. Recently, Huang [3] constructed cryptographic trilinear maps that involve simple, nonordinary abelian varieties over finite fields.

Group-based cryptography has some new direction to offer to answer this question. A bilinear cryptosystem using the discrete logarithm problem in matrices coming from a linear representation of a group of nilpotency class 2 has been proposed in [7].

In this paper, we propose multilinear cryptosystems using identities in nilpotent groups, in which the security is based on the chosen discrete logarithm problem in finite p-groups.

2 Multilinear maps in cryptography

Let n be a positive integer. For cyclic groups G and G_T of prime order p, a map $e : G^n \to G_T$ is said to be a (symmetric) n-linear map (or a multilinear map) if for any

Acknowledgement: The authors were supported by the "National Group for Algebraic and Geometric Structures, and their Applications" (GNSAGA – INdAM). The first author was also partially supported by the ONR (Office of Naval Research) grant N000141512164. This research is also supported by a grant of the University of Campania "Luigi Vanvitelli", in the framework of Programma V:ALERE 2019.

Delaram Kahrobaei, University of York, Deramore Lane, York YO10 5GH, United Kingdom, e-mail: delaram.kahrobaei@york.ac.uk
Antonio Tortora, Dipartimento di Matematica e Fisica, Università della Campania "Luigi Vanvitelli", Caserta, Italy, e-mail: antonio.tortora@unicampania.it
Maria Tota, Dipartimento di Matematica, Università di Salerno, Fisciano (SA), Italy, e-mail: mtota@unisa.it

https://doi.org/10.1515/9783110638387-013

$a_1, \ldots, a_n \in \mathbb{Z}$ and $g_1, \ldots, g_n \in G$, we have

$$e(g_1^{a_1}, \ldots, g_n^{a_n}) = e(g_1, \ldots, g_n)^{a_1 \ldots a_n}$$

and further e is nondegenerate in the sense that $e(g, \ldots, g)$ is a generator of G_T for any generator g of G.

2.1 Fully homomorphic encryption and graded encoding schemes

One of the interesting importance of multilinear maps arises in the notion of one of the revolution which swept the world of cryptography, namely fully homomophic encryption (FHE). The intuition is that FHE ciphertexts behave like the exponents of group elements in a multilinear map, the so called graded encoding scheme [2]. Such a scheme is a family of efficient cyclic groups $G_1, \ldots, G_n$ of the same prime order p together with efficient nondegenerate bilinear pairings $e : G_i \times G_j \to G_{i+j}$ whenever $i + j \leq n$. In other words, if we fix a family of generators g_i of the G_i's in such a way that $g_{i+j} = e(g_i, g_j)$, we can add exponents within a given group G_i,

$$g_i^a \cdot g_i^b = g_i^{a+b};$$

and multiply exponents from two groups G_i, G_j as long as $i + j \leq n$:

$$e(g_i^a, g_j^b) = g_{i+j}^{a \cdot b}.$$

This makes g_i^a somewhat similar to an FHE encryption of a.

2.2 Generalization of multilinear maps to any group

Here, we generalize the definition of a multilinear map to arbitrary groups G and G_T. We say that a map $e : G^n \to G_T$ is a (symmetric) n-linear map (or a multilinear map) if for any $a_1, \ldots, a_n \in \mathbb{Z}$ and $g_1, \ldots, g_n \in G$, we have

$$e(g_1^{a_1}, \ldots, g_n^{a_n}) = e(g_1, \ldots, g_n)^{a_1 \ldots a_n}.$$

Notice that the map e is not necessarily linear in each component. In addition, we say that e is nondegenerate if there exists $g \in G$ such that $e(g, \ldots, g) \neq 1$.

3 Preliminaries

3.1 Nilpotent and Engel groups

A group G is said to be nilpotent if it has a finite series

$$\{1\} = G_0 < G_1 < \cdots < G_n = G$$

which is central, that is, each G_i is normal in G and G_{i+1}/G_i is contained in the center of G/G_i. The length of a shortest central series is the (nilpotency) class of G. Of course, nilpotent groups of class at most 1 are abelian. A great source of nilpotent groups is the class of finite p-groups, that is, finite groups whose orders are powers of a prime p.

Close related to nilpotent groups is the calculus of commutators. Let $g_1, \dots, g_n$ be elements of a group G. We will use the following commutator notation: $[g_1, g_2] = g_1^{-1} g_2^{-1} g_1 g_2$. More generally, a simple commutator of weight $n \geq 2$ is defined recursively by the rule

$$[g_1, \dots, g_n] = \big[[g_1, \dots, g_{n-1}], g_n\big],$$

where by convention $[g_1] = g_1$. A useful shorthand notation is

$$[x, {}_n g] = [x, \underbrace{g, \dots, g}_{n}].$$

For the reader convenience, we recall the following property of commutators:

$$[xy, z] = [x, z]^y [y, z] \quad \text{and} \quad [x, yz] = [x, z][x, y]^z \quad \text{for all } x, y, z \in G. \tag{1}$$

For further basic properties of commutators, we refer to [9, 5.1].

It is useful to be able to form commutators of subsets as well as elements. Let $X_1, X_2, \dots$ be nonempty subsets of a group G. Define the commutator subgroup of X_1 and X_2 to be

$$[X_1, X_2] = \big\langle [x_1, x_2] \,|\, x_1 \in X_1, x_2 \in X_2 \big\rangle.$$

More generally, let

$$[X_1, \dots, X_n] = \big[[X_1, \dots, X_{n-1}], X_n\big]$$

where $n \geq 2$. Then there is a natural way of generating a descending sequence of commutator subgroups of a group, by repeatedly commuting with G. The result is a series

$$G = \gamma_1(G) \geq \gamma_2(G) \geq \dots$$

in which $\gamma_{n+1}(G) = [\gamma_n(G), G]$. This is called the lower central series of G and it does not in general reach 1. Notice that $\gamma_n(G)/\gamma_{n+1}(G)$ lies in the center of $G/\gamma_{n+1}(G)$.

A useful characterization of nilpotent groups, in terms of commutators, is the following.

Lemma 1. *A group G is nilpotent of class at most $n \geq 1$ if and only if the identity $[g_1, \dots, g_{n+1}] = 1$ is satisfied in G, that is, $\gamma_{n+1}(G) = 1$. In particular, in a nilpotent group of class n, the subgroup $\gamma_n(G)$ is central.*

Among the best known generalized nilpotent groups are the so-called Engel groups. A group G is called n-Engel if $[x,_n y] = 1$ for all $x, y \in G$. If G is nilpotent of class n, then G is n-Engel. Also, there are nilpotent groups of class n which are not $(n-1)$-Engel. For example, given a prime p, the wreath product $G = \mathbb{Z}_p \wr \mathbb{Z}_p$ is nilpotent of class p but not $(p-1)$-Engel [4, Theorem 6.2].

Conversely, any finite n-Engel group is nilpotent, by a well-known result of Zorn [9, 12.3.4].

3.2 Nilpotent group identities

The next result is a straightforward application of (1), together with Lemma 1.

Lemma 2. *Let G be a nilpotent group of class $n > 1$ and let a be a nonzero integer. Then, for all $g_1, \dots, g_n \in G$, we have*

$$[[g_1, \dots, g_{n-1}]^a, g_n] = [g_1, \dots, g_n]^a$$

and

$$[g_1, \dots, g_{n-1}, g_n^a] = [g_1, \dots, g_n]^a.$$

Then the following proposition holds.

Proposition 3. *Let G be a nilpotent group of class $n > 1$. Then*

$$[g_1, \dots, g_{i-1}, g_i^{a_i}, g_{i+1}, \dots, g_n] = [g_1, \dots, g_{i-1}, g_i, g_{i+1}, \dots, g_n]^{a_i}, \tag{2}$$

for any $i \in \{1, \dots, n\}$, $a_i \in \mathbb{Z}\backslash\{0\}$ and $g_i \in G$.

Proof. We argue by induction on n. The case $n = 2$ is true by Lemma 2.

Let $n > 2$. Then $G/\gamma_n(G)$ is nilpotent of class $n-1$. Moreover, $\gamma_n(G)$ is central by Lemma 1. Hence the induction hypothesis gives

$$g := [g_1, \dots, g_{i-1}, g_i^{a_i}, g_{i+1}, \dots, g_{n-1}] = [g_1, \dots, g_{n-1}]^{a_i} \bmod \gamma_n(G).$$

It follows that $g = [g_1, \dots, g_{n-1}]^{a_i} h$ where $h \in \gamma_n(G)$. Since $\gamma_n(G)$ is central, applying (1), we get

$$[g, g_n] = [[g_1, \dots, g_{n-1}]^{a_i} h, g_n] = [[g_1, \dots, g_{n-1}]^{a_i}, g_n]$$

and so

$$[[g_1, \dots, g_{n-1}]^{a_i}, g_n] = [g_1, \dots, g_{i-1}, g_i, g_{i+1}, \dots, g_n]^{a_i}$$

by Lemma 2. □

Let G be a nilpotent group of class $n > 1$ and $g_1, \dots, g_n \in G$. According to Proposition 3 for any $a_1, \dots, a_n \in \mathbb{Z}\backslash\{0\}$, we have

$$[g_1^{a_1}, \dots, g_n^{a_n}] = [g_1, \dots, g_n]^{\prod_{i=1}^{n} a_i}.$$

Therefore, we can construct the multilinear map $e : G^n \to G$ given by

$$e(g_1, \dots, g_n) = [g_1, \dots, g_n].$$

Similarly, given $x \in G$, we can consider the multilinear map $e' : G^{(n-1)} \to G$ given by

$$e'(g_1, \dots, g_{n-1}) = [x, g_1, \dots, g_{n-1}].$$

Further, assuming that G is not $(n-1)$-Engel, one can take $x \in G$ in such a way that e' is nondegenerate. In fact, there exists $g \in G$ such that $[x,_{n-1} g] \neq 1$.

4 Multilinear cryptography using nilpotent groups

Here, we propose two multilinear cryptosystems based on the identity (2) in Proposition 3.

4.1 Protocol I

First, we generalize the bilinear map which has been mentioned in [7], to multilinear (n-linear) map for $n+1$ users. Let $\mathcal{A}_1, \dots, \mathcal{A}_{n+1}$ be the users with private exponents $a_1, \dots, a_{n+1}$, respectively. Given an integer $a \neq 0$, the main formula on which our key-exchange protocol is based on, is an identity in a public nilpotent group G of class $n > 1$ (see Proposition 3):

$$[g_1{}^a, g_2, \dots, g_n] = [g_1, g_2{}^a, \dots, g_n] = [g_1, g_2, \dots, g_n{}^a] = [g_1, g_2, \dots, g_n]^a.$$

The users $\mathcal{A}_j$'s transmit in public channel

$$g_i{}^{a_j}, \quad \text{for } i = 1, \dots, n;\ j = 1, \dots, n+1.$$

The key exchange works as follows:

- The user $\mathcal{A}_1$ can compute $[g_1{}^{a_2}, \dots, g_n{}^{a_{n+1}}]^{a_1}$.
- The user $\mathcal{A}_j$ ($j = 2, \dots, n$) can compute

$$[g_1{}^{a_1}, \dots, g_{j-1}{}^{a_{j-1}}, g_j{}^{a_{j+1}}, g_{j+1}{}^{a_{j+2}}, \dots, g_n{}^{a_{n+1}}]^{a_j}.$$

- The user $\mathcal{A}_{n+1}$ can compute $[g_1{}^{a_1}, \dots, g_n{}^{a_n}]^{a_{n+1}}$.

The common key is $[g_1, \dots, g_n]^{\prod_{j=1}^{n+1} a_j}$.

Example: Trilinear cryptography using nilpotent groups of class 3. Let $\mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D}$ be the users with private exponents a, b, c, d, respectively. The users $\mathcal{A}$, $\mathcal{B}$, $\mathcal{C}$, and $\mathcal{D}$ transmit in public channel

$$x^a, y^a, z^a, x^b, y^b, z^b, x^c, y^c, z^c, x^d, y^d, z^d \text{ respectively.}$$

The key exchange works as follows:
- The user $\mathcal{A}$ can compute $[x^b, y^c, z^d]^a$.
- The user $\mathcal{B}$ can compute $[x^a, y^c, z^d]^b$.
- The user $\mathcal{C}$ can compute $[x^a, y^b, z^d]^c$.
- The user $\mathcal{D}$ can compute $[x^a, y^b, z^c]^d$.

The common key is $[x, y, z]^{abcd}$.

4.2 Protocol II

Let G be a public nilpotent group of class $n+1$ which is not n-Engel ($n \geq 1$). Then there exist $x, g \in G$ such that $[x,_n g] \neq 1$. Suppose that $n+1$ users $\mathcal{A}_1, \ldots, \mathcal{A}_{n+1}$ want to agree on a shared secret key. Each user $\mathcal{A}_j$ selects a private nonzero integer a_j, computes g^{a_j} and sends it to the other users. Then:
- The user $\mathcal{A}_1$ computes $[x^{a_1}, g^{a_2}, \ldots, g^{a_{n+1}}]$.
- The user $\mathcal{A}_j$ ($j = 2 \ldots, n$), computes $[x^{a_j}, g^{a_1}, \ldots, g^{a_{j-1}}, g^{a_{j+1}}, \ldots, g^{a_{n+1}}]$.
- The user $\mathcal{A}_{n+1}$ computes $[x^{a_{n+1}}, g^{a_1}, \ldots, g^{a_n}]$.

Hence, again by Proposition 3, each user obtains $[x,_n g]^{\prod_{j=1}^{n+1} a_j}$ which is the shared key.

5 Security and platform group

The security of our protocols is based on the discrete logarithm problem (DLP). The ideal platform group for our protocols must be a non-abelian nilpotent group of large order such that the nilpotency class is not too large and the DLP in such a group is hard.

In [10], Sutherland has studied the DLP in finite abelian p-groups, and showed how to apply the algorithms for p-groups to find the structure of any finite abelian group.

In a series of papers by Mahalanobis, the DLP has been studied for finite p-groups but mostly for nilpotent groups of class 2 [6, 8]. In particular, in [7], Mahalanobis and Shinde proposed p-groups of class 2 in which the platform is not practical as showed by the authors.

Bibliography

[1] Boneh D, Silverberg A. Applications of Multilinear Forms to Cryptography. Contemporary Mathematics. vol. 324. Providence: American Mathematical Society; 2003. p. 71–90.
[2] Garg S, Gentry C, Halevi S. Candidate multilinear maps from ideal lattices. In: EUROCRYPT 2013. LNCS. vol. 7881. 2013. p. 1–17.
[3] Huang MA. Trilinear maps for cryptography. 2018. Preprint available at https://arxiv.org/abs/1803.10325.
[4] Liebeck H. Concerning nilpotent wreath products. Proc Camb Philos Soc. 1962;58:443–51.
[5] Lin H, Tessaro S. Indistinguishability Obfuscation from Trilinear Maps and Block-Wise Local PRGs. In: CRYPTO 2017. 2017.
[6] Mahalanobis A. The Diffie–Hellman key exchange protocol and non-abelian nilpotent groups. Isr J Math. 2008;165:161–87.
[7] Mahalanobis A, Shinde P. Bilinear Cryptography Using Groups of Nilpotency Class 2. In: Cryptography and Coding, 16th IMA International Conference, IMACC 2017. Oxford, UK. 2017. p. 127–34.
[8] Mahalanobis A. The MOR cryptosystem and finite p-groups, Algorithmic problems of group theory, their complexity, and applications to cryptography. In: Contemp Math. vol. 633. Providence, RI: Amer. Math. Soc.; 2015. p. 81–95.
[9] Robinson DJS. A course in the Theory of Groups. 2nd ed. New York: Springer; 1996.
[10] Sutherland AV. Structure computation and discrete logarithms in finite abelian *p*-groups. Math Comput. 2011;80(273):477–500.